



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,584	06/01/2001	Frank W. Sudia	P 264493 AUTH-II	9326
909	7590	06/04/2007		
PILLSBURY WINTHROP SHAW PITTMAN, LLP			EXAMINER	
P.O. BOX 10500			KLIMACH, PAULA W	
MCLEAN, VA 22102				
			ART UNIT	PAPER NUMBER
			2135	
			MAIL DATE	DELIVERY MODE
			06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/870,584

Applicant(s)

SUDIA ET AL.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 February 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 18-21, 72-84 and 109-131 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- ☒ 5) ☒ Claim(s) 19, 75, 76, 81 and 82 is/are ~~allowed~~ objected to.
- 6) ☒ Claim(s) 1, 18, 20-21, 72-74, 77-80, 83-84, and 109-131 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- ☐ Notice of Informal Patent Application
- ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 02/27/07. The amendment filed on 08/01/06 have been entered and made of record.

Response to Arguments

Applicant's arguments filed 02/27/07 have been fully considered.

The applicant argues that the 112 rejections should be withdrawn. This is not found persuasive. The sections indicated by the applicant do not teach the missing parts as disclosed in the 112 rejection.

The applicant argues that Muftic fails to disclose digitally signing said at least one message by which said recipient agrees to said rules, and in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key as recited in claim 1. The combination below of Muftic, Ryder and Miller will overcome these deficiencies.

The newly cited Miller discloses encrypting the public key using the public key of the user so that only that user with the private key can gain access to the public key.

The applicant argues that Ryder does not overcome the deficiencies of Muftic and Curry. This is not found persuasive. The new grounds of rejection below shows the combination of Muftic, Ryder, and Miller teach the limitation of claim 73.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 18-21, 72-78, 116-129 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The applicant claims denying access to public key, and then further discloses "...permitting recipient to utilize public key." In the disclosure the applicant does not disclose denying access to the public key, instead the applicant discloses no one who has not signed the system rules agreement may possess a copy of it (page 36 lines 5-15).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 21, 72-73, 77-78, 116-120, and 129-130 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic (5,745,574) in view of Ryder (4,953,209) and further in view of Miller et al (5,852,666).

Claims 1 and 73: Muftic's patent discloses certifying authority issues digital certificate identifying users of the system in (Fig. 26). Muftic discloses digital certificates being digitally

Art Unit: 2135

signed with a private key of certifying authority to form a digital signature and requiring a public key of certifying authority in order to verify digital signature in (column 14, lines 54-63). Muftic discloses a user transaction in a cryptographic system requires verification by a recipient of user transaction verification based on information in digital certificates and requiring the public key in (column 10 lines 34-49). Muftic discloses providing recipient with at least one message containing the rules of the system including a rule regarding maintaining secrecy of public key in (column 10 lines 52-57). Muftic discloses digitally signing by recipient at least one message (column 11 lines 29-53; column 12 lines 32-40).

Although Muftic discloses authentication, Muftic does not expressly disclose the recipient agreeing to rules and permitting the recipient to utilize the public key and denying access to public key prior to digital signing.

Ryder discloses a system for electronically transmitting data objects such as computer programs with a means for verifying that the computer program was actually received and the terms and conditions of its use accepted by the receiver is presented (abstract). Ryder teaches a receiver (recipient) agreeing to the rules by acceptance of the license agreement terms. When the user agrees to the terms then the electronic object is delivered. It is well known that the process of signing corresponds to acceptance. The user is then provided with the enabling routine after acceptance of the terms (column 8 lines 50 to column 9 line 33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to enable the system when the user agrees to terms as in Ryder in the system of Muftic. One of ordinary skill in the art would have been motivated to do this because it would

Art Unit: 2135

secure electronic data objects and verifying that the objects have been received and accepted which does not require prior authorization for receipt (Ryder column 1 lines 60-67).

However Ryder does not expressly disclose the permitting the use of the public key and denying access to the public key.

Miller discloses a system providing capability security for distributed object system is disclosed (abstract). The system of Miller discloses permitting access to a public key. Only authorized gain access to the object and the encrypted public key (column 9 lines 1-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to control access to the public key as in Miller in the system of Ryder. One of ordinary skill in the art would have been motivated to do this because then the public keys are not made freely available instead they are publicized by their associated objects only on a very restricted basis (Miller column 8 lines 12-21).

Claims 21 and 72: Muftic discloses user transaction is invalid until digital signing is performed in (column 12 lines 22-43).

Claim 77: Muftic discloses user transaction of said recipient in the system is invalid until said digital signing is performed (column 12 lines 30-35).

Claim 78: Muftic discloses responding to said signing by said recipient, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system (column 10 lines 45-57).

Claim 116: wherein the public key becomes inactive after a certain time period, the system further comprising: after the public key becomes inactive, in response to a demonstration

Art Unit: 2135

by the recipient of agreement or consistency with one or more of the rules, activating the inactive public key (Fig 13 and corresponding description).

Claim 117: wherein said demonstration includes information identifying operational capabilities of a secure device and further including information uniquely binding said recipient to said demonstration by the recipient of agreement or consistency with one or more of the rules (column 10 lines 45-57).

Claim 118 wherein the public key is certified by an authority (column 5 lines 20-40).

Claims 119 and 130: wherein said permitting comprises making the public key available by providing access to an inaccessible public key (Fig. 10).

Claim 120 and 129: further comprising: a certifying authority accepting a transaction from the recipient, the transaction based on a transaction of the recipient in the cryptographic system, after demonstration by the recipient of agreement or consistency with one or more of the rules (column 6 lines 1-5 and column 10 lines 50-57).

Claims 18, 20, 74, 121-126, 127-128, and 131 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic (5,745,574) and further in view of Ruftic and Miller as applied in claims 1 and 73 and further in view of Curry (5,940,510).

Claims 18 and 74: Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device.

Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with

Art Unit: 2135

public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 20: Muftic discloses containing rules of system including a rule regarding maintaining secrecy of public key. Muftic does not include a rule to pay for use by said recipient of intellectual property provided through the system. Curry teaches the monetary value of the recipient is decreased (paying) for use of the system when information is matched (rule, column 7 lines 21-35). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a rule to pay as taught in Curry to the system in Muftic in order to provide recipient's privileges and conveniences for the use of the system.

Claim 121 wherein said permitting comprises: in response to a predetermined transaction with a device, activating said public key in said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said device (Fig 13).

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so

Art Unit: 2135

that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 122: wherein a device contains an inactive form of said public key and said permitting comprises activating said inactive public key in said (Fig. 13).

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 123: wherein said permitting comprises transferring said public key to said device.

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 124: wherein said public key is provided in a secure device.

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 125 method further comprising: after said public key becomes inactive, in response to a demonstration by the recipient of agreement or consistency with one or more of the rules, activating said inactive public key in said secure device (Fig. 13).

Claim 126: wherein further including information uniquely binding said recipient to said demonstration by the recipient agreement or consistency with one or more of the rules.

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Art Unit: 2135

Although Muftic discloses policies or rules and authorization privileges Muftic does not expressly disclose the demonstration including information identifying operational capabilities of the device.

Ryder teaches demonstration includes information identifying operational capabilities of the device (column 5 and column 3 lines 56-62).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to confirm that use has received the object agreed upon and agree on the terms and conditions as in Ryder in the system of Muftic. One of ordinary skill in the art would have been motivated to do this because it would remove the need for documents that are normally require registered and signed receipt mail delivery.

Claim 127: said permitting comprises transferring the public key to a secure device, wherein the public key cannot be obtained from the secure device.

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 128: where, in the cryptographic system, a certifying authority issues digital certificates identifying participants of the cryptographic system, the digital certificates being

Art Unit: 2135

digitally signed with a private key of the certifying authority to form a digital signature and requiring a public key of the certifying authority in order to verify the digital signature, and a participant transaction requires verification by a recipient of the participant transaction, the verification based on information in a digital certificate and requiring the public key (Fig. 7 and column 6 lines 1-10).

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 131 wherein said permitting comprises: in response to a predetermined transaction with a device, activating said public key in said secure device, said predetermined transaction including information from the device identifying operational capabilities of the secure device and uniquely identifying said device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said secure device.

Claims 79-80, 83-84, and 109-115 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic (5,745,574) in view of Ryder and Miller and further in view of Curry (5,940,510).

Claim 79: Claim 79 is rejected as claim 1, and further, Muftic's patent discloses certifying authority issues digital certificate identifying users of the system in (Fig. 26). Muftic discloses providing a recipient with a message containing rules of said system (column 10 lines 52-57). This system disclosed by Muftic includes an inactive form of said public key (column 15 lines 32-36 in combination with column 12 lines 60-64). In response to said recipient digitally signing said message, activating said public key in said secure device (column 15 lines 36-43).

Muftic does not specifically disclose providing recipient with a secure device containing public key, wherein public key cannot be obtained from secure device. Curry's patent discloses secure device containing public key, wherein public key cannot be obtained from secure device (column 4 lines 49-55). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ a secure device containing public key wherein public key cannot be obtained from secure device as taught in Curry with public key storage of Muftic in so that the key can be protected and secured at all times against tampering/malicious attacks thus providing secure means to conduct transactions by the users.

Claim 80: Muftic discloses a public key that is a public key of a certifying authority, said providing is performed by a certifying authority (column 10 lines 35-57), said digitally signing comprises hashing said message to obtain a hashed document, digitally signing said hashed document to form a digital agreement (column 12 lines 54-56), and returning said digital

Art Unit: 2135

agreement to said certifying authority, and said activating is performed by said certifying authority (column 12 lines 7-21).

Claim 83: Muftic discloses user transaction of said recipient in the system is invalid until said digital signing is performed (column 12 lines 30-35).

Claim 84: Muftic discloses responding to said signing by said recipient, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system (column 10 lines 45-57 in combination with column 11 lines 60-65).

Claim 109: where, in the cryptographic system, a certifying authority issues digital certificates identifying participants of the cryptographic system (Fig. 3), the digital certificates being digitally signed with a private key of the certifying authority to form a digital signature (part 320 Fig. 3) and requiring a public key of the certifying authority in order to verify the digital signature (column 6 line 65 to column 7 line 20), and a participant transaction requires verification by a recipient of the participant transaction, the verification based on information in a digital certificate and requiring the public key (column 5 lines 5-12).

Claim 110: wherein the public key in the secure device becomes inactive after a certain time period, the method further comprising:

after the public key becomes inactive, in response to a demonstration by the recipient of agreement or consistency with one or more of the rules, activating the inactive public key in the secure device (Fig. 13 and column 10 lines 50-57).

Claim 111: wherein said demonstration includes information from the secure device identifying operational capabilities of the secure device and further including information

Art Unit: 2135

uniquely binding said recipient to said demonstration by the recipient of agreement or consistency with one or more of the rules (10 lines 45-50).

Claim 112: wherein the public key is certified by an authority (column 5 lines 20-40).

Claim 113: further comprising: a certifying authority accepting a transaction from the recipient, the transaction based on a transaction of the recipient in the cryptographic system, after demonstration by the recipient of agreement or consistency with one or more of the rules (column 6 lines 1-5 and column 10 lines 50-57).

Claim 114 wherein the rules comprise a rule regarding maintaining secrecy of the public key (column 10 lines 50-57).

Claim 115: wherein said activating comprises activating said public key in said secure device in response to a predetermined transaction with said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction.

Allowable Subject Matter

Claims 19, 75-76, and 81-82 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Art Unit: 2135

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

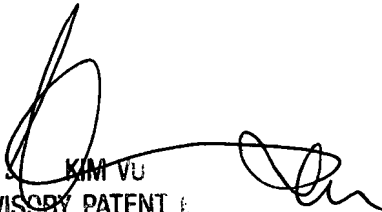
The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK

Saturday, May 26, 2007


KIM VU
SUPERVISORY PATENT &
TECHNOLOGY CENTER 2135